System Security Integrated Through Hardware and firmware (SSITH)

Teaming Profiles

The following information was requested at the SSITH Proposers Day, held on April 21, 2017, and self-reported to the Special Notice inbox. Please see DARPA-SN-17-31 for more information.

While collaborative efforts and teaming are encouraged for the SSITH program, specific content, communications, networking and team formation are the sole responsibility of the proposers. DARPA does not endorse the information and/or organizations listed in the consolidated teaming profile document below and does not vouch for the accuracy of the information, nor does DARPA exercise any responsibility for improper dissemination of the teaming profiles.

SSITH Proposers Day Teaming Profile

Organization: ARM

Name: Eric Hennenhoefer

Title: VP Research

Email: Eric.Hennenhoefer@arm.com

Telephone: 512-789-8360

Mailing Address: 1, 5707 Southwest Pkwy #100, Austin, TX 78735

Website: www.ARM.com

Technical Competencies:

ARM Research has ongoing research projects in the area of hardware, software and system security. This includes future architecture and system architecture for ARM IP (CPUs, GPUs, System IP) as well as technology to better construct IP and SoCs (automation, formal methods, ..)

We interested in discussion teaming opportunities.

ARM IP is broadly available without fee for academic research use Please contact ARM Research and we'll facilitate any requests.

Technical Competencies Sought:

Assured Information Security Inc. (AIS)
Thomas Blake, Operations Manager
blaket@ainfosec.com
315-336-3306, x446
153 Brooks Road, Rome NY 13441
https://www.ainfosec.com/

AIS applicable skills: Hardware-enabled security solutions and "Voice of the Offense" red teaming

AIS' low-level computer architecture group has significant experience in development of hardware-enabled security solutions, including over a decade of performance developing architecture-level protections for workstations, embedded, and mobile devices. AIS has particularly-relevant experience in augmentation of existing computer architectures, including significant past performance developing solutions that protect from both software- and hardware-originating attacks.

As a security research company, AIS has conducted hundreds of embedded system design reviews, application analysis efforts, and secure code reviews to better understand trending technologies and to decrease the overall threats to the system. Most recently the focus has been directed at the embedded systems supporting automobiles, remotely operated or autonomous aircraft, and self-driving military ground vehicles. The embedded platforms supporting the operation of these targets offer communications mechanisms, memory, processors, data storage, and software that may be potentially vulnerable to attack. The expertise possessed by the team is commonly provided to industry leaders and DoD organizations to understand the threats to their system and the potential impact of exploitation.

AIS Relevant Past Performance:

AFOSR GROOM hardware protection research added hardware capabilities to a network interface card of a VM such that the card will not function until the virtual host provides evidence that it has achieved a known, trusted state.

AFRL SecureCore used cooperating software, firmware, and Intel architectural features to apply granular access controls to a workstation's kernel. This effectively composed new architectural features by leveraging Intel's Virtualization Extensions for tasks other than traditional virtual machine isolation.

DARPA High Assurance Cyber Military Systems (HACMS) improved the overall security of embedded systems supporting the operation of autonomous or semi-autonomous air and ground vehicle platforms. AIS serves as the security consultants for HACMS and performs security analyses, code reviews, and design reviews. The AIS red team also exposes other team members to the overall threats in design and implementation that can lead to the compromise of embedded systems.

AFOSR CircuitPUF developed introspective hardware enabling significant new tamper-detection methodologies and an ability to "fight through" the presence of hardware tampering by validating a circuit's internal operating state.

DARPA Ristretto implemented computationally restricted processors using existing Intel CPUs.

AIS facilities include fully equipped hardware, software, microelectronics, FPGA, and PCB development environments. Available lab space operates from secret through SAP accredited levels.

Coherent Logix™

Coherent Logix Company Profile

Contact information:
Coherent Logix, Incorporated
Michael Solka, VP Engineering
solka@coherentlogix.com
512-382-8942

1120 S Capital of Texas Highway
Building 3, Suite 200
Austin, Texas 78746

www.coherentlogix.com

Coherent Logix is a leader in providing programmable processors to our customers in markets and application areas requiring low-power, high-throughput real-time cost effective computing solutions.

Our customers make use of our unique HyperX™ technology, which enables real-time virtualization, to meet converging market requirements. This is driven by the economics of being able to support multiple applications on a single chip and rapidly shrinking product life cycles. The uniqueness of our technology stems from its network memory architecture providing for versatility, extensibility, processing density, heterogeneity, and energy efficiency. It inherently supports massive parallelism through a comprehensive easy-to-use industry standard programming model and software development environment.

Our technology includes a security "toolkit" that allows system designers to construct secure systems based on their specific security requirements. Configurable components of the security toolkit include a secure boot subsystem, a hardware Root of Trust, AES encryption and decryption engines, a hardware random number generator, one-time configurable tamper detection and response mechanisms, secure mechanisms for configuration and real-time control, and integrated key management. Security barriers provide for physical and logical isolation of compute processes.

The Coherent Logix family of high performance, low power secure processors is commercially available today with an integrated system design environment to support development of full applications and secure third party modules. Our product roadmap includes the expansion of the security toolkit to meet the rapidly changing requirements of cybersecurity defense.

Coherent Logix is looking for teaming opportunities on the SSITH program with companies that have advanced systems design expertise (hardware and software). Based on the use of our HyperX secure processors as the core of a high performance secure processing solution, we will work with our partners to develop and field systems that are capable of meeting the SSITH program objectives.

SSITH Proposers Day Teaming Profile

Organization: Florida Atlantic University

Name: Reza Azarderakhsh

Title: Assistant Professor and I-SENSE Fellow

Email: razarderakhsh@fau.edu

Telephone: 561-297-4980

Mailing Address: 777 Glades Road, EE314, Boca Raton, FL 33431

Website: https://faculty.eng.fau.edu/azarderakhsh/

Technical Competencies:

Cryptographic Engineering, Finite Field Arithmetic, Public key cryptography, Elliptic Curve Cryptography, Key Exchange and Authentication, efficient implementations on small and resource-constrained devices (RFIDs, smartcards), fast implementations for high performance applications, hardware (FPGA, ASIC) and software (CPU, ARM, Microcontrollers) implementations. Low power/energy design, silicon area usage optimization, complexity reduction for both time and area. Familiarities with cryptography standardization organizations and relevant documents such as NIST and IEEE,

Technical Competencies Sought:

SSITH Proposers Day Teaming Profile

Organization: MacAulay-Brown, Inc.

Name: Steve Baka

Title: Principal Engineer

Email: stephen.baka@macb.com

Telephone: 540-283-7542

Mailing Address: 4415 Pheasant Ridge Rd, Suite 200, Roanoke VA 24014

Website: www.macb.com

Technical Competencies:

Circuit vulnerability detection & analysis (for exposure to malicious incursion)
Circuit reverse engineering
Trojan circuit detection & analysis
FPGA firmware translation & assessment
Tool and algorithm development for circuit analysis
Secure processing

Technical Competencies Sought:

IC fabrication
Software vulnerability/malice insertion

SSITH Proposers Day Teaming Profile

Organization: NanoLock Security Inc .

Name: Shlomo Oren

Title: Chairman

Email: soren@nanolocksec.com

Telephone: 917-972-1787

Mailing Address: 353 W 56th St. New York , NY 10019

Website: www.nanolocksecurity.com

Technical Competencies:

NanoLock Security Inc. develops an IoT data security platform consisting with a low cost hardware based Access Control System and associated SDK and API . The plaform aims at locking/unlocking any memory device (but specifiaclly NVM) from unauthorized acess ,and thus eliminating any attempt to manipulate with the stored data or firmeware . Our team cosists of ASIC designers , Data security experts , and software engineering .

Technical Competencies Sought:

We are looking for memory and CPU companies to cooperate in the integration of the Platform in their products . We are also looking for IoT device and software providers to cooperate in integration and testing of the platform .

SSITH Proposers Day Teaming Profile

Organization: PARC

Name: Eugene Chow

Title: Principal Scientist and Microsystems Area Manager

Email: echow@parc.com

Telephone: 650-812-4184

Mailing Address: 3333 Coyote Hill, Palo Alto, CA 94306

Website: www.parc.com

Technical Competencies:

-high bandwidth reworkable off-chip interconnects
-theoretical cryptography
-applied cryptography, signal processing, information theory
-network protocols, network security, routing protocols, network time synchronization
-encrypted domain computation
-physical unclonable functions and their security and privacy applications

Technical Competencies Sought:

-integrated circuit design and tools
-chip architecture
-distributed system security (especially information flow control)

SSITH Proposers Day Teaming Profile

Organization: Rensselaer Polytechnic Institute

Name: John F. McDonald

Title: Professor

Email: mcdonald@ecse.rpi.edu

Telephone: 518-276-2919

Mailing Address: Rm. CII 6123, RPI, 110 8th Street, Troy, NY

Website: https://ecse.rpi.edu/index.php/john-mcdonald

Technical Competencies:

VLSI design, especially SiGe HBT BICMOS technology, and most recently acquired CADENCE PDK' s for Global Foundries 22nm SOI and 14nm bulk. Recent work which might be relevant explores a "Lateral SiGe HBT on SOI" device, which at 22nm has THz RF performance and sub picosecond gate delay as well as CMOS compatibility and three orders of magnitude lower power than conventional vertical SiGe HBT's. Extensive microprogramming firmware experience, which includes several courses taught over 44 years. Microprogramming firmware can be sped up using the Lateral SiGe HBT on SOI to accommodate the extra burden of cyber security micro sequences will insure against loss of performance.

Technical Competencies Sought:

DoD partner able to provide interface between university innovations and military applications.

Synopsys Inc. - Teaming Profile

SYNOPSYS®
Silicon to Software

- **Organization: Synopsys Inc. - Mountain View, CA. - www.Synopsys.com**
- **Contacts**
  - Technical: Mike Borza; Synopsys Inc. Technical Member, Solutions Group
    - Mike.Borza@synopsys.com; 613.595.9813; 450 March Road. Suite 401 Ottawa Ontario K2K 3H4 Canada
  - Contracts: Tom Martin; Synopsys Inc. Executive Account Manager
    - Tom.martin@synopsys.com; 443.766.3569; 10440 Little Patuxent Parkway, Columbia, MD

- **Synopsys Technical Competencies and Relevant Facilities**
  - Largest EDA software company by revenue, largest # of R&D personnel including formal technology that could be applied to SSITH
  - Largest, non processor, IP company by revenue, # of engineers and units shipped including robust, widely deployed root of trust, cryptography IP that could be applied to SSITH
  - Fast growing software integrity tool business (Gartner magic quadrant leader) including defensics, fuzzing technology that could be applied to SSITH
  - Leader in hardware and software safety and security in commercial segments (e.g. ISO26262, DO-254, UL 2900)
  - A comprehensive and integrated Verification Continuum platform including simulation, debug, static and formal technology, VIP, Lint, CDC, emulation and prototyping

- **Desired Technical Competencies and Facilities from Other Potential Team Performers**
  - Systems or circuits that could serve as demonstrations or real world examples implementing SSITH innovations in the Aerospace & Defense and Automotive/Industrial markets
  - Knowledge or expertise in machine learning and formal technology as it can be applied to security applications

SSITH Proposers Day Teaming Profile

Organization: Solarflare Communications

Name: Philip Carruthers

Title: Director Federal

Email: pcarruthers@solarflare.com

Telephone: 703 626 8818

Mailing Address: 11773 Hollyview Dr. Great Falls, VA 22066

Website: www.solarflare.com

Technical Competencies:

ASIC Design, Firmware Development, Software Design, Network Controllers, Custom Work, Fabrication, etc. We are an engineering and manufacturing company.

Technical Competencies Sought:

Solarflare is the leading provider of application-intelligent networking I/O software and hardware platforms that accelerate, monitor and secure network data, and is the pioneer in high-performance, low-latency 10/40GbE server networking solutions. With over 1,400 global customers, the company's products are widely used in scale-out server environments such as electronic trading, high performance computing, cloud, virtualization and big data.

Solarflare's software and hardware are available from leading distributors and value-added resellers, as well as from Dell, HP and IBM. Solarflare is headquartered in Irvine, California.

SSITH Proposers Day Teaming Profile

Organization: University of South Florida
Name: Selcuk Kose
Title: Assistant Professor
Email: kose@usf.edu
Telephone: 813 974 6636
Mailing Address: 4202 E. Fowler Ave. ENB118 Tampa Florida 33620
Website: http://www.eng.usf.edu/~kose/

Technical Competencies:

Hardware security, specifically

-- side-channel attacks and related countermeasures

-- Leveraging existing hardware resources as a countermeasure against side-channel attacks including power analysis attacks (SPA, DPA, CPA, LPA, etc) and electromagnetic attacks

-- Developing lightweight countermeasures for IoT devices

-- Co-designing encryption engines with countermeasures

-- Developing combined attacks and related combined countermeasures

-- microarchitectural covert channels

-- Uncovering and mitigating covert channels in modern ICs including SoCs, multi- and many-core platforms, IoT devices, etc

Technical Competencies Sought: